Integrating Critical IT System Development Life Cycle Activities

Building More Secure Systems Through Effective Acquisition and Security Certification Processes

Dr. Ron Ross

National Institute of Standards and Technology

Security Assurance in IT Systems

Building more secure systems requires --

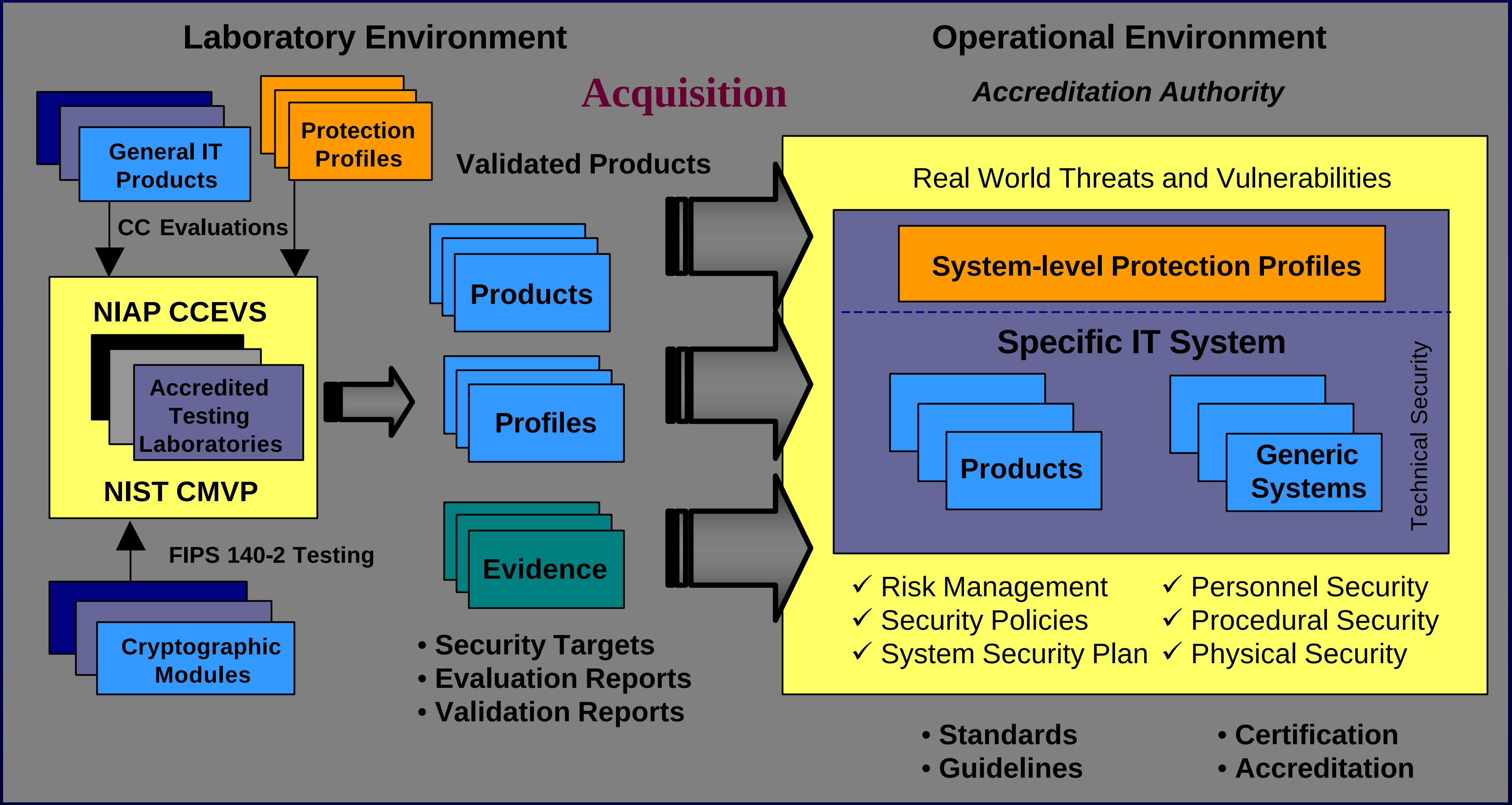
- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

System Development Life Cycle

- Initiation Phase
- Development and Acquisition Phase
- Implementation Phase
- Operations and Maintenance Phase
- Disposal Phase

A Comprehensive Approach

Linking Critical Assessment Activities



Security Certification

"A comprehensive analysis of the technical and non-technical aspects of an IT system in its operational environment to determine compliance to stated enterprise security objectives and requirements…"

- ✓ Achieved through the application of a set of structured activities during and in conjunction with the system life cycle
- ✓ Used to verify the IT system design and to validate a specific implementation for the purpose of identifying risks to unauthorized disclosure, modification, and denial of service of information and resources

System Accreditation

"An official management decision by a designated authority to operate an IT system based on the results of a certification process and other relevant considerations…"

- ✓ Balances mission requirements and the residual risks to the enterprise information system or network after the employment of appropriate protection measures
- ✓ Assigns responsibility for the safe and secure operation of the information system or network to a designated authority

Program Objectives

Phase I

- To develop standardized guidelines for conducting security certifications and accreditations of federal IT systems
- ***Phase II***
- To create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the standardized guidelines

PHASE I

Development of Guidance

- Develop NIST Special Publication 800-37, ***Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems***
- Develop NIST Special Publication 800-37A, *Minimum* ***Security Controls for Information Technology Systems***
- Complete first public drafts by October 2002

SPECIAL PUBLICATION 800-37

Design Goals

- Standardized security certification process for all federal systems
- Flexible and configurable certification tasks targeted to enterprise assurance requirements
- Three levels of security certification for IT systems addressing low, medium, and high risk enterprise environments
- Use national and international IT security standards, whenever possible

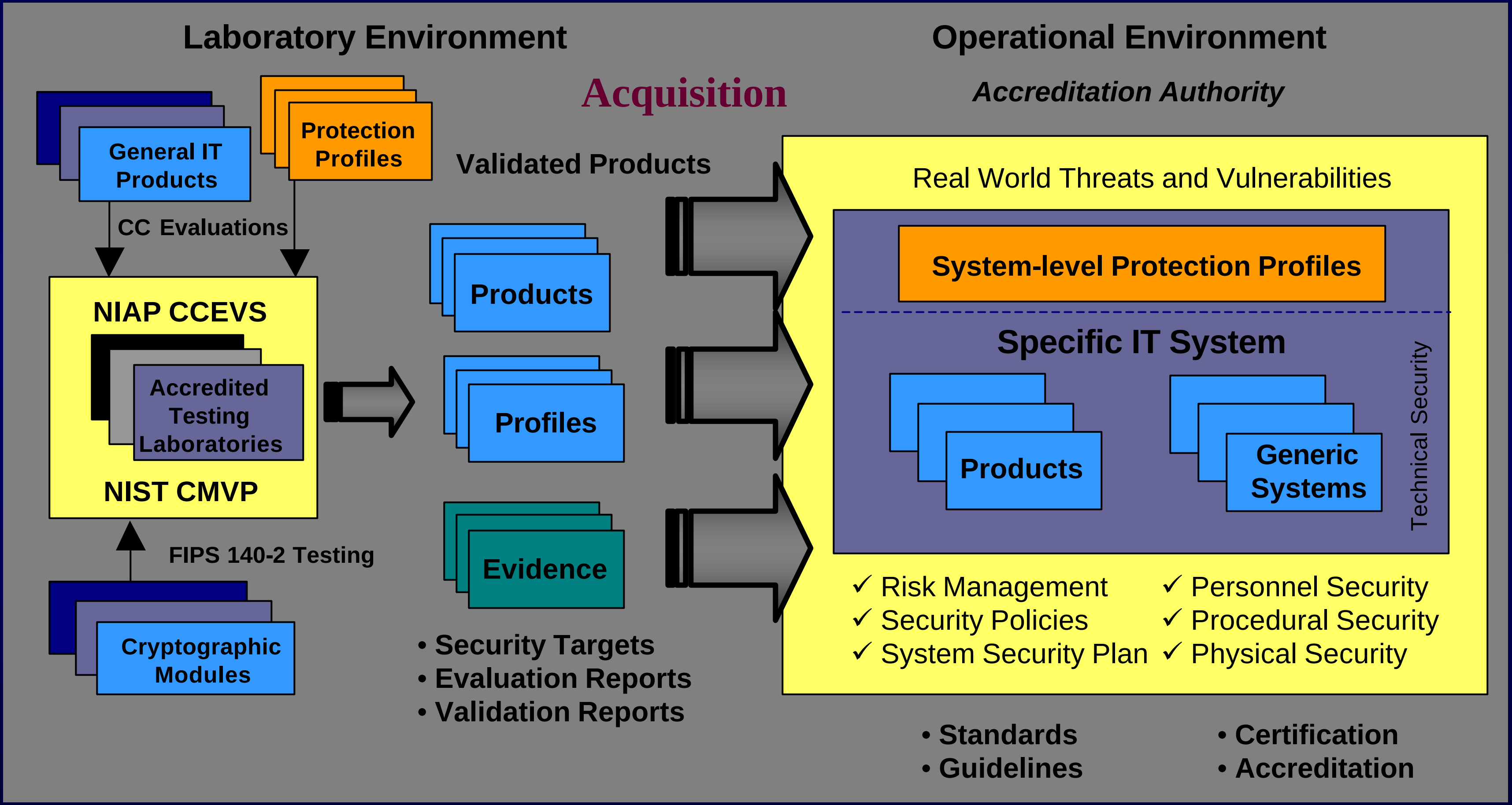
SPECIAL PUBLICATION 800-37A

Design Goals

- Standardized security controls (i.e., management, operational, and technical) for federal IT systems
- Standard package of security controls representing a baseline of security for federal systems in the areas of confidentiality, integrity, and availability
- Optional packages of security controls for increased levels of concern for confidentiality, integrity, and availability

A Comprehensive Approach

Linking Critical Assessment Activities



- Security Targets
- Evaluation Reports
- Validation Reports

- Standards
- Guidelines

- Certification
- Accreditation